UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,979	08/31/2000	Adrian Shields	8490.00	3073

26889 7590 08/28/2006

MICHAEL CHAN
NCR CORPORATION
1700 SOUTH PATTERSON BLVD
DAYTON, OH 45479-0001

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/651,979	SHIELDS, ADRIAN	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 July 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 21-38 are pending.

2. Amendment filed on 07/31/2006 has been received and considered.

Claim Rejections - 35 USC § 112

3. The following rejections under the second paragraph of 35 U.S.C. 112 have been withdrawn based on the filed amendment.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 21-34 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yacobi (US 5878138) and further in view of Menezes et al (Handbook of Applied Cryptography).

As per claims 21 and 33, Yacobi discloses a portable computer, with non-secure user-accessible memory (see column 8 lines 39-49) generating a session key (see column 9 line 47);

encrypting the session key (see column 9 lines 49-50); transmitting the encrypted key to an external terminal (see column 9 lines53-54); receiving and decrypting an encrypted response from the terminal (see column 9 line 65 through column 10 line 31).

Yacobi fails to disclose a) storing records of events experienced by the computer in memory within the computer; and using some of the records as seed for generating plain text of a first session key K1.

However, Menezes et al teaches storing records of events and using the records as a seed for generating a key (see page 172).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Menezes et al's key generation to generate the session key of Yacobi.

Motivation to do so would have been to generate a random bit sequence for a key (see page 171).

As per claims 22, 24, 26-30, and 38, the modified Yacobi and Menezes et al system further includes repeating the above mentioned steps to create a new session key for each new transaction (see Yacobi column 10 lines 38-47) and receiving and decrypting encrypted messaged encrypted by the session key (at

both the portable computer and the external device) (see Yacobi column 9 line 65 through column 10 line 31).

As per claims 23, 25, 31-32, and 34, the modified Yacobi and Menezes et al system further includes the data used as the seed includes at least one element selected from the following group: recorded button selections, recorded pointer movements, recorded data entered by a user, current date setting, and current time setting (see Menezes page 172).

6. Claims 35-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Yacobi and Menezes et al system as applied to claims 21, 24, and 26 above, and further in view of Kawan (US 20020062284).

As per claims 35-37, the modified Yacobi and Menezes et al system fails to include the portable computer requires entry of a Personal Identification Number, PIN, prior to generation of the encryption key, and will not complete the transaction without the PIN

However, Kawan teaches the requirement of a PIN (see paragraph 30).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to require a PIN to perform the actions of the modified Yacobi and Menezes system.

Motivation to do so would have been to verify the user (see paragraph 30).

Response to Arguments

7. Applicant's arguments filed 07/31/2006 have been fully considered but they are not persuasive. Applicant argues Yacobi fails to disclose decrypting the encrypted response using the plain text of K1; Yacobi fails to disclose decrypting; Yacobi fails to disclose an encrypted response; the session key of Yacobi is not used in the encryption of the hash value of the digital cash; the decryption of the hash value is done outside the electronic wallet; there is no motivation to combine because the motivation given is a well known fact; Menezes discusses multiple sources for seeds for random number generation that are not claimed therefore no teaching exists to use a specific one; Menezes teaches against storing the seed in user accessible memory; Menezes requires no memory to perform the generation of the random number; Menezes teaches away from the combination; there is no teaching as to why the "non-anonymous" implementation of Yacobi was selected to be applied to Applicant's claimed invention; a hash value cannot be reversed; EM2 and K2 have not been shown; Yacobi teaches against the use of the system having non secure area; Kawan is insufficient for

showing a PIN is required to complete a transaction; the motivation does not lead to the claimed limitation; no motivation is given as to why to use a PIN for verification; no reasoning as to why one would enter a PIN into a portable device as opposed to directly into the ATM is give; and Yacobi teaches away from entering the PIN into the portable device.

With respect to Applicant's argument that Yacobi fails to disclose decrypting the encrypted response using the plain text of K1, when using a session key to create the secured channel and every message sent through this secured channel during the session is encrypted with the session key. Since the session key is a symmetric key it is used both for encryption on one end of the channel and decryption on the other end of the channel. Also because the bank "decrypts the session key" it is clear that when the session key is used for encryption/decryption it is used in plain text.

With respect to Applicant's argument that Yacobi fails to disclose decrypting as discussed above whenever messages are sent through the secure channel they are encrypted and must be decrypted on the receiving end in order to be read. Therefore Yacobi teaches decrypting. Applicant is thanked for the description of hash functions, however, nowhere was Yacobi relied upon for a teaching of determining the original value of

hashed information (which Applicant has referred to as decrypting).

With respect to Applicant's argument that Yacobi fails to disclose an encrypted response, as discussed above, every message during the session of the secure channel is encrypted using the session key therefore when the "coins 70 are downloaded to the user's electronic wallet 58 over the secure communication channel 68" the "coins" (the bank's response) would be encrypted using the session key.

With respect to Applicant's argument that the session key of Yacobi is not used in the encryption of the hash value of the digital cash, as discussed above, in Applicant's response Applicant alleges that the Examiner relied upon Yacobi to teach that the session key was used to derive the original value of a hash value. This was not what Yacobi was relied upon for, Yacobi teaches the use of a session key to create a secure channel and the session key encrypts the messages transmitted on this secure channel. Some of these messages are hashed values, but the hashed values are encrypted with the session key before being transmitted and decrypted after the reception by the portable device.

With respect to Applicant's argument that the decryption of the hash value is done outside the electronic wallet, this

assertion is incorrect because the electronic wallet must transmit the signed coin to the merchant and since the signed coin had been encrypted by the bank using the session key it must be decrypted by the electronic wallet before being forwarded to the merchant, because the merchant does not have the session key and would have no means to decrypted the encrypted signed coin.

With respect to Applicant's argument that there is no motivation to combine because the motivation given is a well-known fact, the Examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it is well-known to anyone or ordinary skill in the art, as admitted by Applicant, to use random numbers as keys therefore motivation exists to use the random number generation of Menezes to create the keys of Yacobi. Furthermore, it is well known that most keys are pseudorandom and the method of generation taught by Menezes produces random keys.

With respect to Applicant's argument that Menezes discusses multiple sources for seeds for random number generation that are not claimed therefore no teaching exists to use a specific one, Menezes teaches that it is best to use multiple sources to obtain be best random numbers and there is therefore no need to choose a specific source, all or any of them can be used.

With respect to Applicant's argument that Menezes teaches against storing the seed in user accessible memory because as Applicant states "the generator must not be subject to observation", however, Applicant left out one very important point; that this observation is done by an adversary. Therefore there is no teaching against storing the records in user accessible memory.

With respect to Applicant's argument that Menezes requires no memory to perform the generation of the random number, however, as opposed to Applicant's example, the method of Menezes if performed in a computer system and every computer system must have memory. Furthermore even in the analogy given by Applicant memory has to be used because one would have to remember each of the 4 events listed in order to use them as a seed.

With respect to Applicant's argument that Menezes teaches away from the combination because the software approach is "more

difficult" however, the mere fact that it may be "more difficult" does not render the combination non-obvious because as described in the hardware random number generation section, the hardware based generators require either an external device, a further VLSI device, or other tamper resistant devices, while a software based generator does not require any of these devices. Therefore, the software generation has the added benefit of not requiring any of the above-mentioned additional hardware.

With respect to Applicant's argument that there is no teaching as to why the "non-anonymous" implementation of Yacobi was selected to be applied to Applicant's claimed invention, no reasoning is required for choosing one implementation over the other, however, it is clear that the "non-anonymous" implementation more clearly relates to Applicant's invention.

With respect to Applicant's argument that a hash value cannot be reversed, as discussed above, Yacobi was not relied upon to teach the reversing of a hash function.

With respect to Applicant's argument that EM2 and K2 have not been shown as described in Yacobi, "individual keys are used for each transmission and then destroyed" therefore each subsequent sessions between the bank and electronic wallet would

require a new session key which would then encrypt a message to create a new encrypted response.

With respect to Applicant's argument that Yacobi teaches against the use of the system having non-secure area, however as evidence of this Applicant has relied upon a disclosure in Yacobi, which described a different embodiment not relied upon for the rejection of the claims. Yacobi teaches the use of non-secure memory in column 8 lines 39-49.

With respect to Applicant's argument that Kawan is insufficient for showing a PIN is required to complete a transaction because the PIN is not entered through the portable device, however, as described the Kawan when the PIN and/or Biometric ID information is required for verification it is entered on the PDA (see Figure 7 S2).

With respect to Applicant's argument that no motivation is given as to why to use a PIN for verification, Applicant's claim required a PIN to complete a transaction, Kawan teaches this limitation and teaches that a PIN can be used for verification purposes. The mere fact that there can possibly be other methods of verification does not render the motivation improper.

With respect to Applicant's argument that no reasoning as to why one would enter a PIN into a portable device as opposed to directly into the ATM is given, however as described above,

when the PIN and/or Biometric ID information is required for verification it is entered on the PDA (see Figure 7 S2).

With respect to Applicant's argument that Yacobi teaches away from entering the PIN into the portable device, the fact Yacobi teaches traditional verification methods does not teach away from the teachings of Kawan because the Kawan is an improvement on the traditional methods. Therefore combing Kawan with Yacobi improves the Yacobi reference.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER